WHAT IS CLAIMED IS:

1. A method comprising:

comparing first security level information and second security level information, wherein

said first security level information is stored in a security label of a packet received at a network node, and

said second security level information is stored at said network node; and

indicating processing to be performed on said packet based on said comparing.

2. The method of claim 1, wherein

said first security level information represents a first security level, and

said second security level information represents a second security level.

3. The method of claim 2, wherein

said first security level and said second security level implement one of a multi-level security paradigm and a multi-lateral security paradigm.

4. The method of claim 2, wherein

said security label is one of an enumerated security label and a bitmap security label.

5. The method of claim 2, wherein

said second security level is a security level of a port of said network node.

6. The method of claim 5, further comprising:

setting said security level of said port.

7. The method of claim 6, wherein said setting said security level of said port comprises:

storing said second security level in a security label information field of an access control list entry.

8. The method of claim 6, wherein said setting said security level of said port comprises:

storing said second security level in a label range information field of a forwarding table entry.

9. The method of claim 2, wherein said processing comprises:

dropping said packet, if said comparing indicates that said first security level is less than said second security level.

10. The method of claim 2, wherein

said processing comprises at least one of dropping said packet, redirecting said packet and rewriting said security label.

11. The method of claim 1, wherein

said first security level information represents a first security level, and

said second security level information represents a plurality of security levels.

12 The method of claim 11, wherein

said security levels are a range of security levels.

13 The method of claim 12, wherein said processing comprises:

dropping said packet, if said comparing indicates that said first security level is not within said range of security levels.

14. The method of claim 1, further comprising:

storing said second security level information at said network node.

15. The method of claim 14, wherein said storing comprises:

storing said second security level in a security label information field of an access control list entry.

16. The method of claim 14, wherein said storing comprises:
storing said second security level in a label range information field of a forwarding table entry.

17. The method of claim 14, wherein said storing comprises:
communicating said second security level from a first network node by registering said second security level in a context.

18. The method of claim 17, wherein said registering comprises:
updating said second security level information by logically OR'ing third security level information with said second security level information.

19. The method of claim 17, wherein
said context is a generic attribute registration protocol information propagation context, and
said registering said second security level is accomplished by said first network node issuing a join request.

20. The method of claim 14, wherein said storing comprises:
storing said second security level in a label range information field of forwarding table.

21. The method of claim 14, wherein said storing comprises:
storing said second security level in a port of said network node.

22. The method of claim 21, wherein
said port is an egress port.

23. The method of claim 2, further comprising:
determining said first security level.

24. The method of claim 23, wherein said determining comprises:
determining if an ingress port is marked as an access port; and

setting a security level of said ingress port to said first security level, if said ingress port is marked as an access port.

25. The method of claim 24, further comprising:

setting said first security level information to said security level of said ingress port.

26. The method of claim 23, further comprising:

authenticating a user having said first security level, wherein said determining is performed only if said user is authenticated.

27. The method of claim 2, further comprising:

performing said processing on said packet based on said comparing.

28. The method of claim 27, wherein said performing said processing comprises:

forwarding said packet, if said indicating indicates that said packet is allowed to be forwarded; and

dropping said packet, otherwise.

29. The method of claim 27, wherein said performing said processing comprises:

forwarding said packet to a firewall, if said indicating indicates that said packet should be forwarded to said firewall.

30. The method of claim 2, further comprising:

stripping network security information from said packet; and

adding subnetwork security information to said packet.

31. The method of claim 30, wherein

said network security information comprises said first security level information.

32. The method of claim 30, wherein

said subnetwork security information comprises said first security level information.

33. A computer system comprising:

a processor;

computer readable medium coupled to said processor; and

computer code, encoded in said computer readable medium, configured to cause said processor to:

compare first security level information and second security level information, wherein

said first security level information is stored in a security label of a packet received at a network node, and

said second security level information is stored at said network node; and

indicate processing to be performed on said packet based on said comparing.

34. The computer system of claim 33, wherein

said first security level information represents a first security level, and

said second security level information represents a second security level.

35. The computer system of claim 34, wherein said computer code is further configured to cause said processor to:

set said security level of a port, wherein

said second security level is a security level of said port of said network node.

36. The computer system of claim 35, wherein said computer code configured to cause said processor to set said security level of said port is further configured to cause said processor to:

store said second security level in a security label information field of an access control list entry.

37. The computer system of claim 35, wherein said computer code configured to cause said processor to set said security level of said port is further configured to cause said processor to:

store said second security level in a label range information field of a forwarding table entry.

38. The computer system of claim 33, wherein

said first security level information represents a first security level, and

said second security level information represents a plurality of security levels.

39. The computer system of claim 33, wherein said computer code is further configured to cause said processor to:

store said second security level information at said network node.

40. The computer system of claim 39, wherein said computer code configured to cause said processor to store is further configured to cause said processor to:

store said second security level in a security label information field of an access control list entry.

41. The computer system of claim 39, wherein said computer code configured to cause said processor to store is further configured to cause said processor to:

store said second security level in a label range information field of a forwarding table entry.

42. The computer system of claim 39, wherein said computer code configured to cause said processor to store is further configured to cause said processor to:

communicate said second security level from a first network node by virtue of being configure to cause said processor to register said second security level in a context.

43. The computer system of claim 42, wherein said computer code configured to cause said processor to register is further configured to cause said processor to:

update said second security level information by virtue of being configure to cause said processor to logically OR third security level information with said second security level information.

44. The computer system of claim 43, wherein

said context is a generic attribute registration protocol information propagation context, and

said computer code configured to cause said processor to register said second security level is configured to cause said processor to cause said first network node to issue a join request.

45. The computer system of claim 34, wherein said computer code is further configured to cause said processor to:

determine said first security level.

46. The computer system of claim 45, wherein said computer code is further configured to cause said processor to:

authenticate a user having said first security level, wherein

said computer code configured to cause said processor to determine said first security level causes said processor to determine said first security level only if said user is authenticated.

47. The computer system of claim 45, wherein said computer code configured to cause said processor to determine said first security level is further configured to cause said processor to:

determine if an ingress port is marked as an access port; and

set a security level of said ingress port to said first security level, if said ingress port is marked as an access port.

48. The computer system of claim 47, wherein said computer code is further configured to cause said processor to:

set said first security level information to said security level of said ingress port.

49. The computer system of claim 34, wherein said computer code is further configured to cause said processor to:

perform said processing on said packet based on a result generated by said computer code configured to cause said processor to compare.

50. The computer system of claim 49, wherein said computer code configured to cause said processor to perform said processing on said packet is further configured to cause said processor to:

forward said packet, if said computer code configured to cause said processor to indicate indicates that said packet is allowed to be forwarded; and

drop said packet, otherwise.

51. The computer system of claim 34, wherein said computer code is further configured to cause said processor to:

strip network security information from said packet; and

add subnetwork security information to said packet.

52. A computer program product comprising:

a first set of instructions, executable on a computer system, configured to compare first security level information and second security level information, wherein

said first security level information is stored in a security label of a packet received at a network node, and

said second security level information is stored at said network node; and

a second set of instructions, executable on said computer system, configured to indicate processing to be performed on said packet based on said comparing; and

computer readable media, wherein said computer program product is encoded in said computer readable media.

53. The computer program product of claim 52, wherein

said first security level information represents a first security level, and

said second security level information represents a second security level.

54. The computer program product of claim 53, further comprising:

a third set of instructions, executable on said computer system, configured to set said security level of a port, wherein

said second security level is a security level of said port of said network node.

55. The computer program product of claim 54, wherein said third set of instructions comprises:

a first subset of instructions, executable on said computer system, configured to store said second security level in a security label information field of an access control list entry.

56. The computer program product of claim 54, wherein said third set of instructions comprises:

a first subset of instructions, executable on said computer system, configured to store said second security level in a label range information field of a forwarding table entry.

57. The computer program product of claim 52, wherein

said first security level information represents a first security level, and

said second security level information represents a plurality of security levels.

58. The computer program product of claim 52, further comprising:

a third set of instructions, executable on said computer system, configured to store said second security level information at said network node.

59. The computer program product of claim 58, wherein said third set of instructions comprises:

a first subset of instructions, executable on said computer system, configured to store said second security level in a security label information field of an access control list entry.

60. The computer program product of claim 58, wherein said third set of instructions comprises:

a first subset of instructions, executable on said computer system, configured to store said second security level in a label range information field of a forwarding table entry.

61. The computer program product of claim 58, wherein said third set of instructions comprises:

a first subset of instructions, executable on said computer system, configured to communicate said second security level from a first network node comprises a first sub-subset of instructions, executable on said computer system, configured to cause said processor to register said second security level in a context.

62. The computer program product of claim 61, wherein said first sub-subset of instructions comprises:

a first sub-sub-subset of instructions, executable on said computer system, configured to update said second security level information comprises a first sub-sub-sub-subset of instructions, executable on said computer system configure to cause said processor to logically OR third security level information with said second security level information.

63. The computer program product of claim 62, wherein

said context is a generic attribute registration protocol information propagation context, and

said first sub-subset of instructions is further configured to cause said first network node to issue a join request.

64. The computer program product of claim 53, further comprising:

a third set of instructions, executable on said computer system, configured to determine said first security level.

65. The computer program product of claim 64, further comprising:

a fourth set of instructions, executable on said computer system, configured to authenticate a user having said first security level, wherein

said third set of instructions is further configured to cause said processor to determine said first security level only if said user is authenticated.

66. The computer program product of claim 64, wherein said third set of instructions comprises:

a first subset of instructions, executable on said computer system, configured to determine if an ingress port is marked as an access port; and a second subset of instructions, executable on said computer system, configured to set a security level of said ingress port to said first security level, if said ingress port is marked as an access port.

67. The computer program product of claim 66, further comprising:

a fifth set of instructions, executable on said computer system, configured to set said first security level information to said security level of said ingress port.

68. The computer program product of claim 53, further comprising:

a third set of instructions, executable on said computer system, configured to perform said processing on said packet based on a result generated by said first set of instructions.

69. The computer program product of claim 68, wherein said third set of instructions comprises:

a first subset of instructions, executable on said computer system, configured to forward said packet, if said second set of instructions indicates that said packet is allowed to be forwarded; and

a second subset of instructions, executable on said computer system, configured to drop said packet, otherwise.

70. The computer program product of claim 53, further comprising:

a third set of instructions, executable on said computer system, configured to strip network security information from said packet; and

a fourth set of instructions, executable on said computer system, configured to add subnetwork security information to said packet.

71. An apparatus comprising:

means for comparing first security level information and second security level information, wherein

said first security level information is stored in a security label of a packet received at a network node, and said second security level information is stored at said network node; and

means for indicating processing to be performed on said packet based on said comparing.

72. The apparatus of claim 71, wherein

said first security level information represents a first security level, and

said second security level information represents a second security level.

73. The apparatus of claim 72, further comprising:

means for setting said security level of a port, wherein

said second security level is a security level of said port of said network node.

74. The apparatus of claim 73, wherein said means for setting said security level of said port comprises:

means for storing said second security level in a security label information field of an access control list entry.

75. The apparatus of claim 73, wherein said means for setting said security level of said port comprises:

means for storing said second security level in a label range information field of a forwarding table entry.

76. The apparatus of claim 71, wherein

said first security level information represents a first security level, and

said second security level information represents a plurality of security levels.

77. The apparatus of claim 71, further comprising:

means for storing said second security level information at said network node.

78. The apparatus of claim 77, wherein said means for storing comprises:
means for storing said second security level in a security label information field of an access control list entry.

79. The apparatus of claim 77, wherein said means for storing comprises:
means for storing said second security level in a label range information field of a forwarding table entry.

80. The apparatus of claim 77, wherein said means for storing comprises:
means for communicating said second security level from a first network node comprising means for registering said second security level in a context.

81. The apparatus of claim 80, wherein said means for registering comprises:
means for updating said second security level information comprising means for logically OR'ing third security level information with said second security level information.

82. The apparatus of claim 81, wherein
said context is a generic attribute registration protocol information propagation context, and
said means for registering said second security level comprises means for causing said first network node to issue a join request.

83. The apparatus of claim 72, further comprising:
means for determining said first security level.

84. The apparatus of claim 83, further comprising:
means for authenticating a user having said first security level, wherein said means for determining is performed only if said user is authenticated.

85. The apparatus of claim 83, wherein said means for determining comprises:

means for determining if an ingress port is marked as an access port; and

means for setting a security level of said ingress port to said first security level, if said ingress port is marked as an access port.

86. The apparatus of claim 85, further comprising:

means for setting said first security level information to said security level of said ingress port.

87. The apparatus of claim 72, further comprising:

means for performing said processing on said packet, wherein said means for performing said processing uses a result generated by said means for comparing.

88. The apparatus of claim 87, wherein said performing said means for processing comprises:

means for forwarding said packet, if said means for indicating indicates that said packet is allowed to be forwarded; and

means for dropping said packet, otherwise.

89. The apparatus of claim 72, further comprising:

means for stripping network security information from said packet; and

means for adding subnetwork security information to said packet.

90. A network device comprising:

a network interface, wherein

said network interface is configured to receive a packet, and

said network device is configured to store first security level information and to process said packet using said first security level information.

91. The network device of claim 90, wherein said network interface comprises a port, and said port is configured to store said first security level information.

92. The network device of claim 91, wherein said port is an egress port.

93. The network device of claim 91, wherein said network device is further configured to set a security level of said port.

94. The network device of claim 90, wherein said network device is further configured to compare said first security level information and second security level information, wherein said second security level information is stored in a security label of a packet received at said network device; and indicate processing to be performed on said packet based on said comparing.

95. The network device of claim 94, wherein said second security level information represents a second security level, and said first security level information represents a first security level.

96. The network device of claim 95, wherein said network device is further configured to process said packet based on said comparing.

97. The network device of claim 95, wherein said network device is further configured to strip network security information from said packet and add subnetwork security information to said packet.

98. The network device of claim 95, wherein
said first security level is a security level of a port of said network device.

99. The network device of claim 94, wherein
said second security level information represents a second security level, and
said first security level information represents a plurality of security levels.

100 The network device of claim 99, wherein
said security levels are a range of security levels.

101. The network device of claim 95, wherein
said network device is further configured to store said first security level information at said network device.

102. The network device of claim 101, wherein
said network device is further configured to communicate said first security level from a second network device by registering said first security level in a context.

103. The network device of claim 102, wherein
said context is a generic attribute registration protocol information propagation context, and
said registering said first security level is accomplished by said second network device issuing a join request.

104. A network device comprising:
an access control list, wherein
said access control list comprises an access control list entry,
said access control list entry comprises a label information field, and
said label information field is configured to store a security label.

105. The network device of claim 104, wherein
said security label implements a multi-level security paradigm.

106. The network device of claim 104, wherein

said security label implements a multi-lateral security paradigm.

107. The network device of claim 104, wherein said access control list entry further comprises:

a flow label field, wherein

said flow label field allows said access control list entry to be identified as a security labeled access control list entry.

108. The network device of claim 107, wherein said access control list entry further comprises:

a plurality of flow specification fields, wherein

said flow specification fields comprise information identifying processing to be performed on at least one flow.

109. The network device of claim 104, wherein

said security label is configured to be compared to a security label of a packet.

110. The network device of claim 109, wherein said access control list entry further comprises:

a flow specification field, wherein

said flow specification field comprise information identifying processing to be performed on said packet.

111. The network device of claim 110, wherein said access control list entry further comprises:

a flow label field, wherein

said flow label field allows said access control list entry to be identified as a security labeled access control list entry.

112. A network device comprising:

a forwarding table, wherein

said forwarding table comprises a plurality of forwarding table entries, and

at least one forwarding table entry of said forwarding table entries comprises a label range field.

113. The network device of claim 112, wherein said at least one forwarding table entry further comprises:

a port identifier field, wherein

a port identifier stored in said port identifier field identifies a port.

114. The network device of claim 113, wherein

a security label stored in said label range field is associated with said port.

115. The network device of claim 113, wherein said at least one forwarding table entry further comprises:

a media access control (MAC) address field; and

a virtual local area network (VLAN) identifier field, wherein

a combination of said MAC address field and said VLAN identifier field are associated with said port identifier field and said label range field.

116. The network device of claim 113, wherein

said media access control (MAC) address field is configured to store a MAC address,

said VLAN identifier field is configured to store a VLAN identifier,

said VLAN identifier identifies a VLAN, and

a combination of said MAC address and said VLAN identifier identify said port and said security label.

117. The network device of claim 114, wherein said at least one forwarding table entry further comprises:

a media access control (MAC) address field configured to store a MAC address, wherein said MAC address is associated with a security label stored in said label range field.

118. The network device of claim 112, wherein said at least one forwarding table entry further comprises:

a virtual local area network (VLAN) identifier field, wherein

a VLAN identifier stored in said VLAN identifier field identifies a VLAN, and

said VLAN is associated with a security label stored in said label range field.